

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-066

29 January 1980

MEMORANDUM FOR THE RECORD

25X1A
FROM:

[REDACTED]
SECOM Staff

SUBJECT: Meeting with Communications Common Carriers
re FISA Security Procedures

25X1A
1. [REDACTED] Assistant General Counsel, and I participated in meetings at the New York City FBI Field Office on 16 and 17 January 1980 with representatives of communications common carriers to discuss draft security procedures governing assistance they would be required to provide under the Foreign Intelligence Surveillance Act (FISA). Attendees are listed on the attachment.

2. Although many elements of the proposed security procedures were discussed and a number of changes proposed and dealt with during the two days of meetings, most changes were minor and there was no disposition on the carriers' part to try to weaken the security objectives. Development of a final version of the procedures and the full cooperation of the carriers now seems assured.

3. The meeting on 16 January was with representatives of ITT, RCA Global and Western Union (both Domestic and International). They had had little or no experience in electronic surveillances for national security purposes. They did not seem particularly concerned about the draft

Regraded UNCLASSIFIED When
Separate from Attachment

FBI REVIEW
COMPLETED

CONFIDENTIAL

~~CONFIDENTIAL~~

security procedures. Discussion with them was amicable, and largely educational from their perspective. Their questions were answered to their satisfaction. One Q and A merits recording. They asked for explanation of what information it was that the draft procedures said could be extracted and used without classification or secure storage. I answered that this would be telex circuit numbers alone without any notation of intelligence interest, U.S. Government involvement or target identity. Discussion followed about depth of records searches expected of common carriers in order to identify circuit numbers; who in a common carrier could be designated for access to FISA records in a carrier organization that did not have a security officer or department; and on planned procedures for working with common carriers on assistance required under specific court orders. Clarifying changes were discussed and agreed to with respect to the secrecy agreement attached to the security procedures, and to the procedures themselves.

4. Morning and afternoon meetings on 17 January were with representatives of AT&T. While they were in full agreement with the objectives of the security procedures, protracted discussions were necessary to deal with detailed language and administrative changes suggested by them. [] and I had useful conceptual discussions with the AT&T personnel at lunch. During the day we reached agreement on a large number of changes. These are reflected in a new draft prepared by Mr. Kornblum, Department of Justice (copy attached). The general effect of the changes is to make the procedures less of a policy document permitting reasonable flexibility and more of a "how to" manual that can be applied uniformly by people of varying backgrounds. A specific change agreed to was inclusion of language stating that these procedures would be the exclusive security guidance for all matters pertaining to assistance under the FISA. A footnote to this will specify the primacy of these procedures over the Department of Defense Industrial Security Manual. I agreed to contact Defense and advise them of this. Since these procedures have a statutory basis and the Defense ones do not, there can be no meaningful question of which will prevail for FISA matters.

25X1A

5. A subsidiary meeting was held the afternoon of 17 January with the Director of Security for General Telephone ([] participated). The meeting was brief with no issues being raised and the General Telephone representative indicating acceptance of the changes requested by AT&T but questioning the need therefor.

25X1A

~~CONFIDENTIAL~~

6. The presence of [] and myself was very useful to ensure that changes made were consistent with DCI security policy and Community security requirements. The revised draft procedures are now in final coordination looking toward their formal submission to the DCI and the Attorney General for their approval as required by the FISA. We hope for an effective date of mid- or late February 1980.

25X1A

7. [] concurs in this memorandum.

25X1A

Attachments

cc: OGC []

Distribution:

Orig - SECOM Subject w/att
1 - [] w/att
① - SECOM Chrono w/att

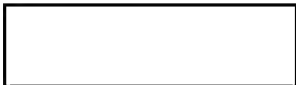
~~CONFIDENTIAL~~

Attendees at 16 and 17 January 1980 Meetings at FBI Field Office, New York City, with Communications Common Carrier Representatives on FISA Security Procedures

Representing:

DCI

25X1A



OGC
SECOM

NSA

25X1A



OGC

Department of Justice

Allan Kornblum

FBI

New York Field Office

Tom McGinnis
Jim Kalstrum
John Schwartz

Headquarters

Irwin Wells
Bill Gore
Billy Spellings
John Kaul

American Telephone & Telgraph

Bill Caming, OGC
Joe Dougherty, Director of Corporate Security
Jack Miller, Chief of Security, New York Bell

25X1

~~CONFIDENTIAL~~



General Telephone

Harry Maynor, Director of Security

International Telephone & Telegraph

Jonathan Lavine, OGC

Jack Anner, Director of Labor Relations & Security

RCA Global

George Stepanenko, OGC

Bob Sanders

John Stackhouse

Western Union (Domestic)

Ernest Walton, OGC

Fred Gordon

Western Union International

Bob Michelson, General Counsel

STATINTL

SECURITY PROCEDURES FOR
SAFEGUARDING RECORDS PERTAINING TO ELECTRONIC
SURVEILLANCE WITHIN THE UNITED STATES AUTHORIZED
UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Section 1 - General Provisions

a. These security procedures are approved by the Attorney General and the Director of Central Intelligence pursuant to Section 102(a)(4)(B) and Section 105(b)(2)(C) of the Foreign Intelligence Surveillance Act of 1978 (the "Act"). Communication common carriers and affiliates thereof providing information, facilities, or technical assistance needed by the Federal Bureau of Investigation (FBI) to accomplish electronic surveillances authorized by the United States Foreign Intelligence Surveillance Court (the "Court") pursuant to Section 105 of the Act, or by the Attorney General pursuant to Section 102 of the Act, shall maintain all records concerning the surveillance or the aid furnished the FBI, including records created by the Court, the executive branch, and the carriers or affiliates, in accordance with these procedures.* These procedures provide exclusive security guidance for all matters pertaining to assistance under the Act.**

b. All appropriate records concerning a surveillance or aid furnished the FBI, including Court orders and Attorney General directives requiring assistance, shall be stored in GSA-approved safes or safe-type steel file containers (Class VI or better) having a built-in, three position, dial-type changeable combination lock.

*These procedures also shall apply to landlords, custodians, and other specified persons providing information, facilities, or technical assistance pursuant to Section 105(b)(2)(C) of the Act. The terms "common carrier" and "affiliates" are intended to apply, wherever they appear in these procedures, to landlords, custodians and other specified persons as well.

**The procedures and requirements contained in the Department of Defense's Industrial Security Manual for Safeguarding Classified Information, which regulates and governs the handling of classified information maintained by Department of Defense and other Federal Government contractors, are not applicable to the safeguarding of classified FISA orders and related records concerning surveillances and aid furnished thereunder which the carrier may wish to retain.

c. Records shall not be copied or removed from secure premises, except as provided in Sections 2 or 3 of these procedures, and then only such limited information a communication common carrier or affiliate may require in order to render the assistance directed may be extracted from the records.

d. Communication common carriers may transmit classified material only as follows:

(1) Top Secret material shall be transmitted by hand by appropriately cleared personnel or by such other means as the FBI may authorize;

(2) Secret and Confidential material shall be transmitted in the manner specified in subsection 1d(1) above or by registered mail within U.S. Postal Service channels; and

(3) All classified material being transmitted shall be double wrapped with the inner envelope marked to show the classification of the contents.

e. All personnel of communication common carriers or affiliates who will have access to classified information, or who can reasonably associate assistance activities with surveillances conducted pursuant to the Act, shall first undergo background investigations by the FBI under standards commensurate with the classification of the materials to which they will have access, as set out in Director of Central Intelligence Directive 1/14, 13 May 1976, Executive Order 10450, or successor directives. Such personnel will not be provided access to classified information unless and until they have been granted appropriate security clearances by an authorized designee of the Attorney General and the Director of Central Intelligence.* In emergency circumstances when, as determined by the Special Agent in charge of the appropriate FBI Field Division Office, or his designee, the time required to obtain clearances would cause failure or unreasonable delay in conducting a surveillance, an uncleared person may be granted access to classified information and such authorization shall be confirmed in writing to the

*The Director of Security of the Department of Justice is designated to issue such security clearances.

- 3 -

communication common carrier. All personnel having access to classified information shall sign the security agreement form attached hereto as soon as practicable.

f. If a question concerning the security clearances of communication common carrier personnel is raised subsequent to the granting of a clearance, the matter shall be referred to the FBI, which shall advise the clearing authority who will take such action as may be appropriate.

g. Communication common carriers shall advise the appropriate FBI Field Office whenever any cleared employee no longer has a need for clearance in connection with matters pertaining to the Act.

h. The FBI, in consultation with the communication common carriers, shall provide such security briefings for cleared personnel as the FBI deems appropriate.

i. If necessary for the sole purpose of providing assistance, the telephone or circuit numbers or other information identifying the subject of a surveillance may be provided to communication common carrier personnel who do not have security clearances under circumstances in which the numbers or other information cannot reasonably be associated by such personnel with surveillances under the Act.

j. Violations of these procedures shall be promptly reported to the FBI. The FBI shall determine and report the facts and circumstances of such violations to the Attorney General and the Director of Central Intelligence.

k. Except as otherwise provided in these procedures surveillance records and information contained therein shall not be provided or disclosed to any other person except as may be required by legal process* and then only after prior notification to the Attorney General.

l. Nothing in these procedures shall preclude the disclosure of unclassified information related to assistance under the Act to the chief executive officer of a communication common carrier by cleared carrier personnel when necessary for the effective administration or the continuation of assistance provided by the communication common carrier.

*As used herein the term "legal process" shall include sealed orders issued by the U.S. Foreign Intelligence Surveillance Court.

Section 2 - Carrier Storage

Communication common carriers or affiliates wishing to store records containing classified information under their direct control may do so under the following procedures:

- a. Except as provided in paragraph 1. i. records maintained or created by a communication common carrier or affiliate thereof shall be marked with the same security markings (i.e., classification, authority therefor, duration thereof and action to be taken at the end of the duration period) or other documents bearing on electronic surveillances covered by the Act.
- b. All such records shall be stored in facilities meeting the physical security standards for safes or safe-type steel file containers as provided in subsection 1. b. of these procedures. The combination of the container shall be known only to specifically designated security department personnel who qualify under the standards described in subsection 1. e. above. Combinations shall be changed whenever a person in authorized possession is relieved of responsibility therefor, and in any event at least once a year. Storage containers shall be accessible only to designated security department personnel.
- c. Secure rooms or spaces in which containers are located shall be so equipped as to preclude surreptitious entry without detection, such as by being equipped with appropriate volumetric or perimeter alarm systems or safe alarm systems to signal forced entry or entry after normal entry portals have been locked. Where deemed necessary by the Government, and when the communication common carrier or affiliate has an acceptable guard force, alarms shall alert the carrier or affiliate guard force capable of responding within five (5)* minutes; otherwise such alarms shall signal FBI field offices, local law enforcement agencies or alarm companies in the city or locality in which the carrier or affiliate is located. Such arrangements shall be made with the cooperation of the FBI which shall insure that local law enforcement or the alarm company is aware of the significance of an alarm signal and the necessity for a prompt response

*Required in U.S. Intelligence Board Directive D-9 1/20.
paragraph 13B

- 5 -

thereto. When the facilities within which secure storage containers are located are unoccupied by security department personnel all entry portals shall be locked and alarms activated. Compliance with the requirements of this paragraph (2C) shall be based upon a survey to be conducted by the FBI at each storage site. A report of each survey shall be made to the Attorney General and the Director of Central Intelligence or their designee.*

d. Access to surveillance records shall be limited to specifically designated supervisory Security Department personnel or other appropriate personnel who have a need to know, (not to exceed five (5) in total number unless approved by the FBI) at the location where the records are stored. In addition, a senior official of a communication common carrier designated by the carrier, the General Counsel of the carrier and any attorney of that carrier or affiliate thereof specifically designated by the General Counsel shall, when having an express need-to-know and appropriate security clearances as described in subsection 1. e. above, be granted access to such records through the specifically designated Security Department personnel herein before described.

e. The designated security department personnel shall be responsible for ensuring that these security procedures are followed. They shall establish and maintain a system of records control and accountability sufficient to identify receipt, reproduction, access, dissemination and destruction of classified documents. Such accountability system shall be open to inspection by the FBI upon request.

*The Director of Security of the Department of Justice is hereby authorized to review such survey reports, to determine compliance with these procedures.

Section 3 - Trust Receipt

Communication common carriers or affiliates not wishing to store records containing classified information under their immediate control may store them with the government under the following procedures:

a. Except as provided in Section 2 of these procedures all classified information concerning a surveillance or aid furnished the FBI, including Court orders and Attorney General directives requiring assistance, shall be stored in GSA-approved safes or safe-type steel file containers (as described in Section 1(b) of these procedures) maintained within FBI field offices.

b. The FBI shall provide communication common carriers or affiliates with a trust receipt for all records maintained at Bureau field offices on their behalf. Such receipts shall not contain any classified information. Carriers shall be provided full access to the records for which the trust receipt is provided during normal business hours or at any other mutually convenient time.

c. Records stored on behalf of communication common carriers or affiliates providing assistance shall not be copied or removed from FBI field offices, except that such limited information a carrier or affiliate may require in order to render the assistance directed may be extracted from the records. The information will be contained in a Court order directed to the communication common carrier or in an Attorney General directive to the carrier.

d. Notwithstanding subparagraph 3c above a communication common carrier or affiliate which is capable, or becomes capable, of maintaining records in accordance with the security provisions of Section 2 may remove at its discretion, after providing reasonable notice to the FBI, records containing classified information stored on its behalf, including secondary Court orders and Attorney General directives, provided that such records are stored by the carrier or affiliate in strict accordance with these security procedures. Upon termination of the assistance provided with respect to a particular surveillance, all documents containing classified information may be returned, at the option of the communication common carrier or affiliate, for storage at FBI field offices under a trust receipt.

- 7 -

Section 4 - Effective Date

These procedures shall be effective as of _____ provided that, if deemed necessary by an authorized designee of the Attorney General and the Director of Central Intelligence, the effective date of these procedures may be deferred or these procedures may be modified for a reasonable and temporary period not exceeding 90 days to permit communication common carriers or affiliates thereof to establish security facilities meeting the requirements of these procedures. Any such temporary deferral or modification shall provide for reasonable alternative procedures to ensure security for information involved.

COMMUNICATION COMMON CARRIER EMPLOYEE
SECURITY AGREEMENT WITH THE U.S. GOVERNMENT
PURSUANT TO THE FOREIGN INTELLIGENCE
SURVEILLANCE ACT OF 1978

I understand that in the course of my employment with the (company name) I may be given access to information pursuant to the Foreign Intelligence Surveillance Act that is classified in accordance with the standards set forth in Executive Order 12065, as amended or superseded. I further understand that the unauthorized disclosure of such information might jeopardize the foreign intelligence and counterintelligence activities of the United States government. In consideration of my being given access to such classified information, and the special trust and confidence placed in me by the (company name) and the United States government, I accept the following responsibilities:

1. I agree that during my employment with the (company name), and at all times thereafter, I will never disclose such classified information that I have obtained during the course of my employment with the company; and I agree to comply with all of the obligations contained in Security Procedures for Safeguarding Records Pertaining to Electronic Surveillance Within the United States Authorized Under the Foreign Intelligence Surveillance Act of 1978.

2. I agree that during my employment with the (company name) and at all times thereafter, I will never disclose or publish in any form or any manner, except as authorized by the said Security Procedures, any information related to a specific surveillance conducted pursuant to the Foreign Intelligence Surveillance Act, except under lawful process after due notice to the Attorney General or the Director of Central Intelligence, or with the express written approval of the Attorney General or the Director of Central Intelligence.

ILLEGIB

possession, or for which I am responsible because of my employment with the company, upon demand by an appropriate company official or upon the conclusion of my employment with the (company name). I understand that all classified information which I may acquire in the course of my employment with the company, which fits the descriptions set out in paragraph 1 and 2 of this agreement, ~~are~~^{is} and will remain the property of the United States Government.

- 2 -

4. I further understand that violations of the above mentioned security procedures may result in the termination of any security clearance I may have and continued access to classified information, may result in administrative sanctions, and may subject me to civil liability or criminal prosecution.

WITNESSED

SIGNED

DATE

TRUST RECEIPT NO. _____

Date _____

The undersigned hereby acknowledges receipt of the records concerning a surveillance or aid furnished the FBI by [communication common carrier or affiliate] in accordance with court orders or Attorney General directives issued pursuant to the Foreign Intelligence Surveillance Act. Such records are identified below by docket number or other appropriate designation.

1. Court Order, Docket No. _____, Issued By Judge _____, on (Date) _____.
2. Court Order, Docket No. _____, Issued By Judge _____, on (Date) _____.
3. Attorney General Certification No., _____, (Date) _____.
4. Attorney General Certification No., _____, (Date) _____.

In consideration of such receipt and other valuable considerations, the undersigned agrees to hold such records in trust for the [communication common carrier or affiliate] and to provide full access to these records to its authorized representatives during normal business hours or at any other mutually convenient time. The undersigned further assumes full responsibility to act as trustee for the carrier in maintaining the security of the documents and preventing alteration or destruction of them.

Date_____
SAC, FBI Field Office

WITNESS: _____